19MAG4785

ORIGINAL

Approved: _____
LOUIS A. PELLEGRINO
Assistant United States Attorney

Before: THE HONORABLE STEWART D. AARON
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA	:	**SEALED COMPLAINT**
	:	
- v. -	:	Violations of
	:	18 U.S.C. §§ 1343,
DEJAN MEDIC,	:	1028A and 2.
	:	
Defendant.	:	COUNTY OF OFFENSE:
	:	NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

MEGAN A. DOLAN, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE
(Wire Fraud)

1. From at least in or about July 2018, up to and including at least in or about March 2019, in the Southern District of New York and elsewhere, DEJAN MEDIC, the defendant, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, knowingly would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, MEDIC received and attempted to receive wire transfers that were induced from victim businesses through fraudulent emails and phone calls.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT TWO
(Aggravated Identity Theft)

2. From at least in or about July 2018, up to and including at least in or about March 2019, in the Southern District of New York and elsewhere, DEJAN MEDIC, the defendant, knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, MEDIC impersonated individual company executives in connection with the offense charged in Count One of this Complaint.

(Title 18, United States Code,
Sections 1028A(a)(1), 1028A(b), and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

3. I am a Special Agent with the FBI, and I have been personally involved in this matter. This affidavit is based upon my investigation; my conversations with law enforcement agents, witnesses, and others; and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview of the Scheme

4. Based on my experience and involvement in this investigation, a Business Email Compromise ("BEC") scheme is a scheme by which a target impersonates company employees through the use of spoofed corporate email accounts, to defraud the company or its employees, customers, or vendors of money.

5. Based on my involvement in this investigation, and as discussed in further detail below, I know the following:

a. Since approximately January 2019, the FBI has been investigating a BEC Scheme which has used fraudulent phone calls and spoofed email correspondence to obtain money from at least fifteen victim businesses in the United States (the

"Victim Companies"), including at least one located in the Southern District of New York, by impersonating the senior management of the Victim Companies' European-based parent companies.

b. The scheme is typically initiated through a telephone call to the U.S.-based Victim Company from a European telephone number. During this call, the caller poses as either a senior executive or a board member of the Victim Company's parent company, utilizing the name and title of a real individual known to the U.S.-based Victim Company (the "Phony Telephone Call").

c. During the Phony Telephone Call, the caller will request the Victim Company's assistance with a purportedly urgent wire transfer of funds. For example, the caller will ask that the Victim Company remit a payment for debts owed by the Victim Company's parent company in Europe.

d. After the Phony Telephone Call, the Victim Company receives an initial follow-up email from an email address with a domain name that is either the same, or misleadingly similar to, the Victim Company's foreign parent company email, a process known as email "spoofing."

e. Following this initial conversation, the sender of the spoofed email typically transitions away from the spoofed email account by inserting one of five email accounts (the "BEC Email Accounts") into the conversation, which are accounts that have been established with the same well-known commercial email service. Sometimes the sender of the spoofed email informs the Victim Company that his corporate email is having problems, and therefore that future correspondence should be with the BEC Email Account.

f. Using this process, the user of the BEC Email Account then corresponds with the Victim Company regarding the payment of the alleged debts that the Victim Company's European parent purportedly owes. This correspondence includes wire transfer information, and frequently results in tricking the Victim Company into paying the purported debts of their European parent via wire transfers to accounts controlled by a member of the scheme.

Victim-1

6. Based on my review of statements made by representatives of a U.S.-based subsidiary of a real estate investment firm headquartered in London, United Kingdom, with offices throughout Europe, and a U.S.-based subsidiary with an office in New York, New York ("Victim-1"), bank records, and email correspondence, I have learned the following:

a. A Manhattan-based Vice President of Victim-1 (the "Vice President") reported that on or about the morning of July 19, 2018, he received a phone call purporting to be from the Luxembourg-based chief financial officer ("CFO") of Victim-1's parent company.[1] Acting as the CFO, the caller stated that he had an urgent matter for which he needed Victim-1's assistance. The caller then stated, in sum and substance, that there was a deal closing that day, and that he needed to pay a vendor. The caller stated that if the vendor was not paid immediately, the European parent company of Victim-1 would have to pay a penalty, or risk losing the deal. The caller then told Victim-1's Vice President that banks were already closed in Europe, and that he needed Victim-1's assistance to pay using banks located in the United States.

b. Later that day, at approximately 11:36 a.m. Eastern Standard Time (EST), the Vice President received an email at his work email address that purported to be sent from the CFO's work email in Luxembourg. This was a spoofed email, in which, among other things, the sender changed the parent company's legitimate email format from ".com" to ".lu," to imply that the email had originated from Luxembourg. The spoofed email requested that the Vice President wire approximately $143,750.09 to a corporate bank account located in Croatia.

c. At approximately 11:46 a.m. EST, the perpetrator then sent a follow up email to the Vice President using the email address "deuschland.gmbh00@[redaction 1].com"[2] ("Email Address-1," one of the BEC Email Accounts). The subject line of

---

[1] The Vice President reported to me that the actual CFO of the parent company was known to him, and the caller impersonated the CFO with a Germanic accent and certain mannerisms, such that the Vice President believed that he was dealing with the actual CFO of Victim-1's parent company.

[2] The Government has redacted words that would identify the service provider from the email address at issue.

the email contained contact details, providing Email Account-1 as the email that the Vice President should use going forward. The Vice President then notified his supervisor, who initiated two wire transfers, for approximately $100,000 and $43,750.09, to the corporate wire address that the perpetrator provided in Croatia.

d. Thereafter, Email Address-1 sent at least four additional follow up emails to the Vice President, to check on the status of the wire transfers.

e. The following day, the Vice President received a follow up email from the ".lu" spoofed email account, purporting to contain reimbursement information from the European-based parent company to its U.S.-based subsidiary, but this reimbursement information later proved to be false. Subsequent correspondence induced Victim-1 to send another wire of approximately $23,760 to the same corporate account in Croatia.

DEJAN MEDIC's Involvement in the BEC Scheme

7. Through FBI interviews with at least fifteen Victim Companies, email correspondence, bank records, and my review of non-content information obtained about the BEC Email Accounts through a Court Order issued pursuant to 18 U.S.C. § 2703(d), I have learned the following:

a. The Victim Companies have been defrauded using the same or similar methods, typically linked by, among other things, use of one the five linked BEC Email Accounts. For a majority of the Victim Companies, correspondence with victims was diverted to deutschland.swissag@[redaction 1].com ("Email Account-2," one of the BEC Email Accounts). Based on non-content data obtained from the provider of the BEC Email Accounts, each of the five BEC Email Accounts were linked by cookies, indicating that they were all accessed by the same Internet browser, and therefore controlled by the same user.

b. For at least seven of the Victim Companies, rather than provide a corporate account as the recipient for the wire transfer, email correspondence provided the name DEJAN MEDIC, the defendant, as the intended recipient of the fraudulently induced wire transfer.

8. From my conversations with other law enforcement agents, my review of investigatory files, and conversations with

foreign law enforcement authorities in Hungary, I have learned the following:

a. DEJAN MEDIC, the defendant, opened multiple bank accounts in his name in Hungary using real identification documents and a photograph of himself (the "Hungarian Bank Accounts"). Based on my understanding of Hungarian banking requirements, the Hungarian Bank Accounts were opened in person by MEDIC.

b. At least four Victims Companies were fraudulently induced to send funds directly to the Hungarian Bank Accounts, which were confirmed by Hungarian authorities as having been opened and controlled by MEDIC.

9. Through my discussions with other law enforcement agents, my review of statements made by representatives of a Swiss manufacturing company with a U.S.-based Victim subsidiary ("Victim-2"), bank records, my review of investigatory files and conversations with foreign law enforcement authorities in Hungary, I have learned the following:

a. Through correspondence with Email Account-2, Victim-2 was fraudulently induced to wire funds into an account controlled by a precious metal company.

b. After it realized that it had been a victim of fraud, Victim-2's European parent company enlisted law enforcement in Europe in an attempt to retrieve or claw back the stolen funds, but according to Victim-2, those law enforcement sources informed Victim-2, in sum and substance, that the funds could not be returned back because they had been converted into gold.

c. On or about April 27, 2019, DEJAN MEDIC, the defendant, was arrested by Hungarian authorities attempting to cross the border into Serbia in possession of, among other things, three serialized gold bars.

10. Based upon my review of statements made by representatives of the Victim Companies, email correspondence, and bank records, I have learned that between at least in or about June 2018, through at least in or about March 2019, at least fifteen Victim Companies have suffered a total loss of approximately $3.7 million through the course of the scheme. In addition, the investigation has revealed that the scheme has also attempted to obtain approximately $6.8 million in

additional fraudulent payments from U.S.-based Victim Companies that were unsuccessful.

WHEREFORE, deponent respectfully requests that a warrant issue for the arrest of DEJAN MEDIC, the defendant, and that he be arrested, and imprisoned or bailed, as the case may be.

Megan A. D

MEGAN A. DOLAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
16th day of May, 2019

THE HONORABLE STEWART D. AARON
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK